REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
25-10-2016	Final Report	15-Aug-2015 - 14-Aug-2016

4. TITLE AND SUBTITLE
Final Report: A Laboratory for Characterizing the Efficacy of Moving Target Defense

5a. CONTRACT NUMBER
W911NF-15-1-0512

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS
Kun Sun

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
College of William and Mary
P.O. Box 8795

Williamsburg, VA 23187 -8795

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
66772-CS-RIP.2

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
Under ARO funded BAA project entitled “Modeling and Analysis of Moving Target Defense Mechanisms in MANET”, we at College of William and Mary are developing a scalable, dynamic, adaptive security system that combines virtualization, emulation, and mutable network configurations to thwart the malicious scanning procedure from obtaining the real system infrastructure. One major challenge is to meet our scalability goal with the resource constraints of a small number of servers, and making virtual nodes “real enough” from the view of attackers. Unfortunately, with our existing resources, we are only able to implement small-scale prototypes of the proposed

15. SUBJECT TERMS
Moving Target Defense, software defined networking, testbed

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kun Sun
UU	UU	UU	UU		19b. TELEPHONE NUMBER 757-221-3457

Report Title

Final Report: A Laboratory for Characterizing the Efficacy of Moving Target Defense

ABSTRACT

Under ARO funded BAA project entitled "Modeling and Analysis of Moving Target Defense Mechanisms in MANET", we at College of William and Mary are developing a scalable, dynamic, adaptive security system that combines virtualization, emulation, and mutable network configurations to thwart the malicious scanning procedure from obtaining the real system infrastructure. One major challenge is to meet our scalability goal with the resource constraints of a small number of servers, and making virtual nodes "real enough" from the view of attackers. Unfortunately, with our existing resources, we are only able to implement small-scale prototypes of the proposed capabilities, mostly consisting of a single server running the software we developed, and multiple client machines interacting with it. Such prototypes have been fundamental to demonstrate the feasibility of our approach, but a larger scale and more realistic implementation is needed to thoroughly vet the proposed framework and direct future research and development towards demonstrating cloud-wide scalability of our solution. This ARO DURIP addresses the equipment costs of servers, storage, network switches, and workstations, and it enables us to fully integrate all the proposed capabilities, realistically assess the efficacy of our research, and get valuable feedback from the analysts. Additionally, it offers our students the opportunity to gain precious hands-on experience from low-level system development to high-level cloud configuration that is extremely important to DOD missions.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Nothing to report.

Graduate Students

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Post Doctorates

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Faculty Supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME	PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

See Attachment.

Technology Transfer

Nothing to report.

"A Laboratory for Characterizing the Efficacy of Moving Target Defense"

Awarding Agency: US Army Research Office
Contract #: ARO W911NF-15-1-0512

Final Report
Reporting Period: 15 August 2015 – 14 August 2016

Principal Investigator: Dr. Kun Sun
Department of Computer Science,
College of William and Mary
McGrothlin-Street Hall, #105
College of William and Mary
Williamsburg, VA 23187
E-Mail: ksun@wm.edu
Phone: (757) 221-3457
Fax: (757) 221-1717

1 Statement of the Problem

Under ARO funded BAA project entitled "Modeling and Analysis of Moving Target Defense Mechanisms in MANET", we at College of William and Mary are developing a scalable, dynamic, adaptive security system that combines virtualization, emulation, and mutable network configurations to thwart the malicious scanning procedure from obtaining the real system infrastructure. A novel aspect of this project is the virtual machine (VM) based large-scale network containers that increase the attack surface by hiding the real system in a large number of decoys. One major challenge is to meet our scalability goal with the resource constraints of a small number of servers, and making virtual nodes "real enough" from the view of attackers. Resource multiplexing techniques and emerging hardware support can help us achieve the scalability goal with undistinguishable decoys.

Unfortunately, with our existing resources, we have been able to implement only small-scale prototypes of the proposed capabilities, mostly consisting of a single server running the software we developed, and multiple client machines interacting with it. Such prototypes have been fundamental to demonstrate the feasibility of our approach, but a larger scale and more realistic implementation is needed to thoroughly vet the proposed framework and direct future research and development towards demonstrating cloud-wide scalability of our solution. To this end, we proposed the acquisition and building of an infrastructure for characterizing the efficacy and security of the proposed network-based moving target defense framework. This ARO DURIP addresses the equipment costs of servers and network switches to build a software defined networking infrastructure, which enables us to fully integrate all the proposed capabilities, realistically assess the efficacy of our research, and get valuable feedback from the analysts. Additionally, it offers our students the opportunity to gain precious hands-on experience from low-level system development to high-level cloud configuration that is extremely important to DOD missions.

2 Summary of Important Results

2.1 Test-bed Environment

We build an SDN test-bed for deploying and testing the proposed decoy-based MTD framework at a much larger scale, as shown in Figure 1. It consists of two Dell PowerEdge R730 Server [1], two Dell Networking S6000 ethernet switches [3], five Dell Networking S4048 ethernet switches [4], and two Dell Networking N1524 switches [2]. To isolate our test-bed from the campus network but still enable the remote access, we connect the R730 servers to the campus routers. Our research experiments comprise a large of number of virtual machines (VMS) that are typically memory-intensive and computation-intensive. The powerful PowerEdge

R730 servers have Intel Xeon E5-2603 processors to provide sufficient computation power. The total amount of RAM provided by the two servers is 2048 GB, which provides us the flexibility to build large scale virtual networks. Dell Networking N1524 switches are used to form the control plane of the software defined network. Two high-end S6000 switches and five low-end S4048 switches provide enough flexibilities and resources for performing various experiments in a small-size SDN test-bed.

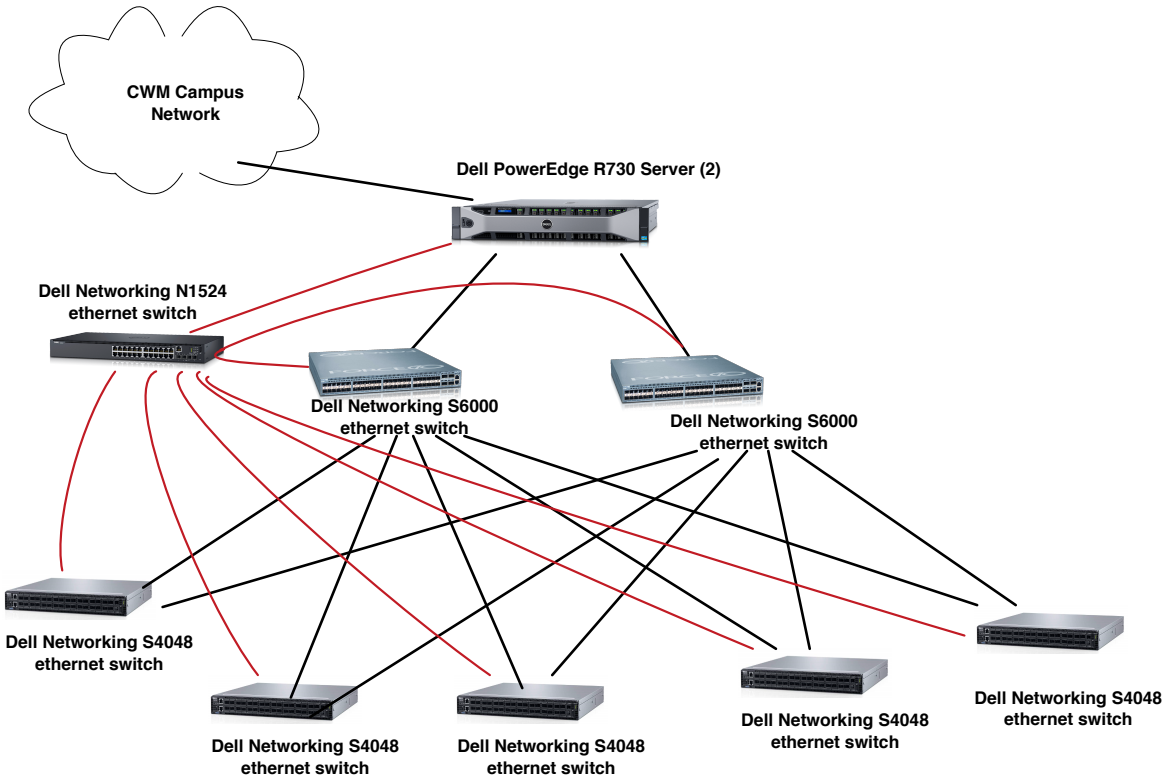

Figure 1. Test-bed Architecture of private SDN for the study of MTD techniques

2.2 Impact on Research

The test-bed supports two research projects that perform experiments and collect research results on the test-bed.

2.2.1 Non-intrusive Dual-Phase System Call Reduction in Application Containers [5]

Linux containers have recently gained more popularity as an operating system level virtualization approach for running multiple isolated OS distros on a control host or deploying large scale microservice-based applications in the cloud environment. The wide adoption of containers as an application deployment platform also attracts attackers' attention. Though a number of security mechanisms have been proposed to enhance the container security, only coarse-grained configuration settings are provided, and it lacks a framework to customize the container protection for a specific application. In this paper, we propose a container security

mechanism called IPA that can dramatically reduce the number of system calls of a given application container by customizing and differentiating its necessary system calls at two different phases, namely, booting phase and running phase. For a given application container, we first trace its invoked system calls at booting phase and running phase, respectively. Then we extend the seccomp filtering kernel security feature to dynamically configure the available system calls when the application is running at two different phases. Our mechanism is non-intrusive to the application running in the container. We apply IPA to several most popular web server and data store application containers from Docker hub, and the experimental results show that it can reduce more than 50% and 35% system calls for the data store and the web server application containers with negligible performance overhead. The Dell R730 servers provide the computation power to conduct the research experiments in this work.

2.2.2 Camouflaging Critical Server Infrastructures with Large Scale Decoy Farm [6]

Traditional deception-based cyber defenses often undertake reactive strategies that utilize decoy systems or services for attack detection and information gathering. Unfortunately, the effectiveness of these defensive mechanisms has been largely constrained due to the low fidelity of the decoys, the poor scalability of the decoy deployment platform, and the static nature of the decoy configurations. Attackers greatly benefit from the unsophisticated decoy design, which allows them to identify the existence of decoys and bypass the prescribed security measures. To overcome this disadvantage, we propose a defensive framework that can proactively protect critical servers against targeted remote exploitation based attacks that are typically preceded by persistent network reconnaissance. We have designed a highly scalable system that seamlessly integrates a large number of high fidelity decoys with the critical server infrastructures. Specifically, we have incorporated three major functions into our system: (1) creating a hybrid decoy platform consisting of lightweight proxies backed by dedicated high-fidelity decoy servers; (2) agile traffic steering and load balancing among the proxies together with dynamic proxy network configuration shuffling; (3) transparent network connection translation in order to maintain those pre-existing alive connections during the shuffling process. We evaluate the effectiveness of our approach in defending against remote exploitations and show that our system introduces negligible performance overhead in our software defined networking test-bed.

2.3 Impact on Research-Related Education

The impact of the SDN test-bed infrastructure on research-related education and the expected benefits for our student population are twofold. First, students directly involved in a wide range of security related projects, including the aforementioned ARO BAA effort, are able to ground their research in reality. In fact, they are given the opportunity to deploy and test their algorithms and data structures in realistic scenarios, where they have to work as part of an integrated system, rather than in isolation, and operate on live network traffic. This opportunity is extremely valuable for Ph.D. students pursuing an academic career and seeking to validate the feasibility of their research ideas.

Second, students pursuing a career outside the academia in areas important to national defense are able to leverage the in-house availability of such an SDN infrastructure as a golden training opportunity, which provides them with a solid understanding of current open problems

and available solutions. Additionally, they become familiar with all the issues that arise when deploying and integrating novel solutions and research prototypes in a real-world environment, thus gaining the hands-on experience that industry demands.

2.3.1 Impact on Existing Facilities

The Computer Science Department at the College of William and Mary maintains a state-of-the-art computing environment for experimental research and education. It maintains a modern network of Linux workstations for research and instructional labs. Also, the College has received an NSF Major Research Infrastructure grant for the establishment of a Computational Science Cluster to foster collaboration between the sciences at William and Mary and to provide a significant computational resource in the form of the SciClone cluster. The department has eight Xeon compute servers with a total of 200 cores that are available for all the faculties and students. The SDN test-bed is compatible with the existing facilities, and they are easily integrated into the department's IT systems. Furthermore, they extend our research capability on performing experimental studies of security and privacy in a fully controlled privacy cloud environment.

The servers and switches in the test-bed are located in the university's IT machine room in Jones Hall, where the machine room not only provides the necessary cooling and power system, but has a backup generator. As Dell's main server line, the R730 servers are expected a lifespan of 10+ years with the capability of obtaining replacement parts for the servers.

3 Reference

[1] Dell PowerEdge R730 Rack Server, http://www.dell.com/us/business/p/poweredge-r730/pd

[2] Dell Networking N1524 Switches, http://www.dell.com/us/business/p/networking-n1500-series/pd

[3] Dell Networking S6000, http://www.dell.com/learn/us/en/45/shared-content~data-sheets~en/documents~dell_networking_s_series_s6000_spec_sheet.pdf

[4] Dell Networking S4048, http://www.dell.com/learn/us/en/04/shared-content~data-sheets~en/documents~fy16q1_201_dell_networking_s4048-on_specsheet_040215.pdf

[5] Lingguang Lei et al., "Non-intrusive Dual-Phase System Call Reduction in Application Containers", under submission to security conference.

[6] Jianhua Sun et al., "Camouflaging Critical Server Infrastructures with Large Scale Decoy Farm", under submission to security conference.